Developing an Efficient Solution to Information Hiding through Text Steganography Along with Cryptography

[1]Venkata Bhanu Chowdary Allada, [2]Mallikarjun Susarla
[1,2]Dept. of CSE, GITAM University, India

Abstract
Now-a-days information security over unsecured channel is the most challenging issue. Most of the proposed algorithms in network security include only cryptography. Although cryptanalysis takes a lot of time to get back the plain text, the security given is not efficient in the conditions where the plain text is more important than the time. Therefore, we have proposed an efficient solution to use steganography along with cryptography for increased security. The proposed algorithm involves the pure format based text steganography along with the secret key cryptography. The cover text is made as ordinary as possible. The plain text from the sender is encrypted using DES algorithm which generates the cipher text. This cipher text is then embedded into the cover text using the embedding algorithm which generates the stego text which is sent through the unsecured channel. The receiver then receives the stego-text converts it into the cipher text using extraction algorithm which is then converted back to plain text using DES decryption. Instead of correct recipient if any third party or cracker or hacker obtains the stego text they may think that it is an ordinary text to teach English to the kids since we made it like that or if they try to extract the original message it requires a huge amount of computational time.
The changes that can be made to the proposed algorithm is that we can make use of AES algorithm instead of DES algorithm since AES make use of 128-bit key and DES uses 64-bit key and increase in key length provides greater security.

Keywords
Cryptography, Steganography, Increased Security, DES, AES, Cover Text, Cipher Text

I. Introduction

Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message i.e. Steganography and the other changes the message itself i.e. Cryptography. In this paper we propose a new technique in which Cryptography and Steganography are used as integrated part. The following paper first encrypts the plain text to cipher text using one of the existing algorithm available in the market. Once the Cipher Text is generated, the Cipher text with the cover text is used to create a stenographic text also known as stego-text. A cover text is a normal text behind which the original message is made hidden. The stego-text generated is sent to the destination. Now even if the intruder taps the network channel and try to read the message out of it, the only thing he could try to read is the cover text. The Intruder thinks that the cover text is the original message which was sent over network, but actually the original message was hidden behind the cover text. This makes the data secure even if the link was captured by the third party intruders. For converting the plain text to cipher text we will use the DES algorithm. DES is a 64-bit encryption algorithm which defines more secured message transfer over the network with much higher computational time to break the code. Steganography is the practice of concealing an image or file within another image or file. Various techniques include pin punctures, typewriter correction ribbons, watermarking. One text can be used to hide another text. This is known as text steganography. We make use of text steganography in this process.
If in a case the intruder comes to know about the use of Steganography and Cryptography for the message encryption, all he could do is get the cipher text which is already encrypted with the best algorithm available and it takes a lot of computational time to break the code. This process is shown in frig. 1 briefly.

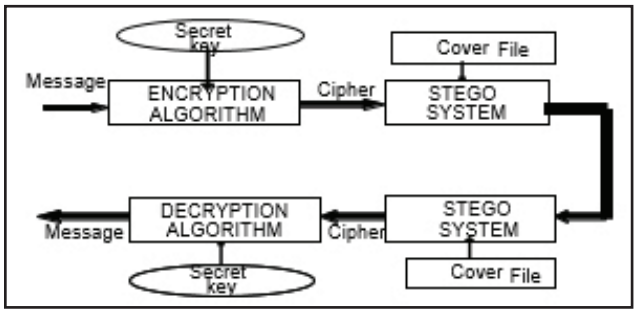

Fig. 1: Text Steganography Along with Cryptography

II. System Analysis

A. Existing System

Information hiding has always been a complicated task, even though many solutions and techniques have been implemented they are not efficient enough and always had some drawbacks. Many cryptographic systems have been proposed for security purposes. One of the most used cryptographic system is Data Encryption Standard (DES). DES is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit cipher text by means of permutation and substitution. The process involves 16 rounds and can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied. For any cipher, the most basic method of attack is brute force, which involves trying each key until you find the right one. The length of the key determines the number of possible keys and hence the feasibility of this type of attack. DES uses a 64-bit key, but eight of those bits are used for parity checks, effectively limiting the key to 56-bits. Hence, it would take a maximum of 2^56, attempts to find the correct key.

B. Proposed System

The proposed technique for information hiding through the format-based pure text steganography is divide d into a cascade of two processes. They are the preparation of the ordinary cover text and the embedding process. Embedding the secret message into the cover text the stego-text is transmitted over the unsecured communication channel. At the intended receiver the extraction process applied to extract the secret message sent by the sender is also discussed here.

B. Proposed System

The proposed technique for information hiding through the format-based pure text steganography is divide d into a cascade of two processes. They are the preparation of the ordinary cover text and the embedding process. Embedding the secret message into the cover text the stego-text is transmitted over the unsecured communication channel. At the intended receiver the extraction process applied to extract the secret message sent by the sender is also discussed here.

1. Preparation of Cover Text

The cover text has been made explicitly in such a way that it looks like an ordinary text consisting of all the English characters which are mostly used to teach English to the kids. The cover text has been treated as a linear array of 224 English characters stored from position 0 to 223.

2. Embedding Process

First, then embedding process takes the prepared cover text which is treated as a linear array of English characters. Secondly, taking the original message the process encrypts it by DES encryption with a secret key of 56 bit. Then counting the frequency with respective positions of each encrypted character in the cipher text, the algorithm retrieves the position of each encrypted character comparing with the characters of the cover text. Treating each of the positions as an ASCII it takes the equivalent character of each ASCII and thus the algorithm conceals each encrypted character to this newly retrieved character from the cover text. Finally, an alphanumeric puzzle using the counted frequency with respective positions of each character in the cipher text and the characters, which conceal the encrypted characters, is added at the end of the cover text. In the puzzle, each finally retrieved character is placed directly. Each position guided by the frequency count of each encrypted character in the cipher text is split into two integers so that the position can be represented by some arithmetic operations and then the operations are added in the puzzle section. The stego-text is sent to the receiver over the unsecured communication channel.

Embedding Algorithm

The pseudo-code of the embedding algorithm is illustrated below:

(i). Input the cover text.
(ii). Input the original message to be embedded.
(iii). Encrypt the original message with DES encryption.
(iv). Count the frequency with respective positions of each character in the cipher text.
(v). Retrieve the position of each encrypted character comparing with the characters of the cover text and treating each of the positions as an ASCII take the equivalent character of each ASCII
(vi). Make an alphanumeric puzzle:
(a). Spilt each position guided by the frequency count into two integers
(b). Directly place the final retrieved character and place some arithmetic operations performing by the two split integers.
(vii). Add the puzzle at the end of the cover text.

3. Extracting Process

In the extraction phase, first the counted frequency with respective positions of each character in the cipher text and the characters, which conceal the encrypted characters, are retrieved from the alphanumeric puzzle of the stego-text. Taking the equivalent ASCII value of the characters from the puzzle the characters stored in the positions equivalent to the ASCII are retrieved. Then, each of the characters is placed to those positions mentioned by the frequency count with respective positions in the cipher text. Then the DES decryption is applied to the retrieved cipher text to get the original message sent by the sender.

Extracting Algorithm

The pseudo-code of the extracting algorithm is illustrated below:

(i). Input the stego-text.
(ii). Input the alphanumeric puzzle from the stego–text and do:
(a). Retrieving the character from the puzzle take the equivalent ASCII of each character.
(b). Retrieve the character from the text of the position equivalent to the calculated ASCII.
(iii). Retrieve the frequency an d associated positions of each character from the puzzle and combine all the characters according to the frequency and positions.
(iv). Decrypt the combined text with DES decryption.

III. Implementation

A. Embedding

1. Input the Cover Text

The cover text consists of a title, digits, lowercase letters, uppercase letters, punctuatons, operators and special characters. For the developed text steganographic algorithm the ordinary cover text is shown in Table 1 below.

Table 1: Overtext as a Linear Array

Character	Position
I	0
n	1
.	-
0	53
.	-
a	81
.	-
~	223

2. Input the original message to be embedded.

Let the original message to be embedded be P = First Australia Next Japan.

3. Encrypt the original message with DES encryption.

After performing DES encryption using a 16-digit hexadecimal key, K=AD0B6594EC1320DF gives C=0x134ba6386e73d2 dc76e546e5076bea6da90dce72296c4c4 2de6a3472464b01f9 chiphertext.

4. Count the frequency with respective positions of each character in the cipher text.

Now, the algorithm counts the frequency of each character in the chiphertext and also stores the positions as in a Table.

5. Retrieve the position of each encrypted character comparing with the characters of the cover text and treating each of the positions as an ASCII take the equivalent character of each ASCII

6. Make an alphanumeric puzzle:

- Spilt each position guided by the frequency count into two integers.
- Directly place the final retrieved character and place some arithmetic operations performing by the two split integers.

7. Add the puzzle at the end of the cover text shown in Table 2 below.

Table 2: Alphanumeric Puzzle

Characters that conceal the message	Arithmetic operations denoting the frequency with respective positions
5	0+0=0, 23+3=26, 6*6=36, 64-2=62
h	1+0=1
.	.
V	66-2=64

B. Extraction

1. Input the stego-text.

In the extraction phase, the algorithm first takes the stego- text as the input.

2. Input the alphanumeric puzzle from the stego–text and do:

First, the algorithm takes the first part, consisting of only characters, of the alphanumeric puzzle from the stego-text. Then, the algorithm takes the equivalent ASCII value of each character. It finds the encrypted and concealed character of that position from the stego-text which is equal to the calculated ASCII. In our example, if the retrieved character is '5', its equivalent ASCII value is 53 and thus '5' is replaced by '0', which was concealed, because '0' is placed at position 53 in the stego-text.

3. Retrieve the frequency an d associated positions of each character from the puzzle and combine all the characters according to the frequency and positions.

Now, the algorithm takes the second part of puzzle section which contains the arithmetic operations. The output of each arithmetic operation in each row indicates the positions of each finally retrieved character for the same row. Then, the algorithm places the character in those positions. For example, the output of 0+0=0, 23+3=26, 6*6=36, 64-2=62 contains the position 0, 26, 36 and 62 for character '5' and '5' is equivalent to '0' as by step 2. So, '0' is placed in positions 0, 26, 36 and 62. This is shown in Table 3 below.

Table 3: Retrieving of Frequency

Puzzled character	5	h	6	.....	V
Equivalent ASCII of the character	53	104	54	.....	86
Retrieved Character	0	x	1	.....	f
Arithmetic Operation	0+0=0, 23+3=26, 6*6=36, 64-2=62	1+0=1	2+0=2, 66-3=63	.....	66-2=64
Frequency	4	1	2	.....	1
Positions against frequency	0, 26, 36, 62	1	2, 63	.....	64

4. Decrypt the combined text with DES decryption.

Finally, the DES decryption with the same key as used in the encryption phase is applied to the combined text to get the original message, P = First Australia Next Japan.

IV. Result

The performance study with the results of the experiments of the proposed method has been presented here. For both data hiding and data extracting the algorithm has been implemented by a simple JAVA program. The proposed algorithm has also been evaluated for its accuracy using different sets of sample data. The comparison of the developed steganography with other methods is shown below. Thus it is clear that the steganographic model offers a higher level of security. In most of the existing methods the size of the cover text is very bulky. But for our proposed method the comparative size of the cover text is very smaller as it is not system generated and interactively very simple. Thus, it ensures high transfer speed shown in Table 4 below.

Table 4. Comparison With Other Methods

	Proposed Method	GATS [20]	wbStego [21]	SNOW [22]	Stego [23]
Use of encryption/ decryption key	Yes	Yes	Yes/No	Yes/No	Yes
Cover file	Not system generated but simple and interactive	System generated	Not system generated	Not system generated	Not system generated
File types	.txt	.txt	Image, pdf, txt	-	-
Visibility of secret message	Not visible	Not visible	Not visible	Visible	Not visible
Type of Encryption	DES-Data Encryption Standard with 64 bit key	Playfair	Various	ICE-Information Concealment Engine with 64 bit key	-

Moreover, none of the cover text or the steganographic algorithm will not be easily available for various steganographic attacks like the known carrier attack, known message attack, steganography only attack, known steganography attack, or statistical attack. Hackers or crackers can proceed to extract the secret message with only the stego-text, but it requires a huge computational time. However, the developed algorithm can be applied in various security systems such as E-mail communication system, cloud based system, banking security system, mobile communication system, key or password management system, administrative security system, network security system, etc.

V. Conclusion

In this project it is mainly used for hiding the data in audio files and sends the data in secure manner in audio file. So the hackers can't access the data. In the receiver side LSB algorithm extract the text from the audio file. Using the AES Algorithm, we decrypt the data form the encrypted format.

When compared to DES algorithm, AES is more secured and since AES uses 128-bit encryption strategy. The AES encryption with text steganography will make the system passive to attackers. Even if the attacker gets hold of the stego text, it will be quite difficult for the intruder to decrypt the AES encryption as it will take more time with brute force. It is quite impossible that the intruder can ever get hold of the message with AES encryption.

Another Enhancement to the existing project can be made as with the introduction of video steganography. Video steganography with AES encryption is totally a new level of encryption.

References

[1] Cryptography and Network Security: Principles and Practice, William Stallings, Prentice Hall, New Jersey.

[2] Introduction to cryptography, Johannes A. Buchmann, Springer- Verlag.

[3] Cryptography and Network Security, AtulKahate, TMH

[4] Documentation of Java Swing (Java Swing Official documentation)
[5] https://www.fourmilab.ch/javascrypt/stego.html
[6] https://en.wikipedia.org/wiki/Steganography
[7] http://bit.ly/1oTMjDi
[8] https://en.wikipedia.org/wiki/NetBeans
[9] www.wseas.us/e-library/conferences/2008/hangzhou/.../116-586-634.pdf
[10] www.ijraonline.com/Published%20Papers/1(1)31-35.pdf
[11] S.Changder, N.C. Debnath, D. Ghosh, "LCS based Text Steganography through Indian Languages" Proceedings of 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010), IS 978-1-4244-5539-3, pp. 53-58(vol 8) July, 2010, Chengdu, China.
[12] A.Alabish, A. Goweder, and A. Enakoa, A Universal Lexical Steganography Technique, International Journal of Computer and Communication Engineering, Vol. 2, No. 2, March 2013, pp. 153-157.
[13] N. Rani and J. Chaudhary, Text Steganography Techniques: A Review, International Journal of Engineering Trends andTechnology (IJETT), Volume 4, Issue 7- July 2013, pp. 3013-3015.
[14] A. K. Hmood, H. A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, On the Capacity and Security of Steganography Approaches: An Overview, Journal of Applied Sciences, Vol. 10(16), pp. 1825-1833, 2010.
[15] L. Y. POR and B. Delina, Information Hiding: A New Approachin Text Steganography, 7th WSEAS Int. Conf. on AppliedComputer & Applied Computational Science (ACACOS), Hangzhou, China, April 6-8, 2008, pp. 689-695
[16] W. Bender, D. Gruhl, N. Morimoto and A. Lu, Techniques for data hiding, IBM Systems Journal, Vol. 35, Nos. 3 & 4, 1996.
[17] D. Baudran, H. Gilbert, L. Granboulan, H. Handschun, A. Joux, P. Nguyae, F. Noilhan, O. Poincheva, T. Pornin, G. Poupard, J. Sternand S. Vaudenay, Report on the AES Candidates, Proc. of the 2nd ASE Conference, Rome, Italy, 1999.